ThunderX, Ranzy Locker

id-ransomware.blogspot.com/2020/08/thunderx-ransomware.html

ThunderX Ransomware

Ranzy Locker Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью Salsa20, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: ThunderX. На файле написано: нет данных.

Обнаружения:
DrWeb ->
Trojan.Encoder.32480, Trojan.Encoder.32485, Trojan.Encoder.32806, Trojan.Encoder.33314
BitDefender -> Trojan.GenericKD.34388567, Gen:Heur.Ransom.Imps.1
ESET-NOD32 -> A Variant Of Win32/Filecoder.ODD, A Variant Of Win32/Filecoder.RanzyLocker.A
Malwarebytes -> Ransom.FileCryptor, Ransom.Ranzy
Microsoft -> Trojan:Win32/Ymacco.AA64, Ransom:Win32/FileCrypter.MB!MTB
Rising -> Trojan.Generic@ML.85 (RDML:***, Ransom.FileCrypter!8.11F42 (TFE*
Symantec -> ML.Attribute.HighConfidence, Downloader, Ransom.RanzyLocker
TrendMicro -> Trojan.Win32.WACATAC.THHAHBO, Ransom.Win32.THUNDERX.SMTH

© Генеалогия: Ako ⇒ ThunderX > Ranzy Locker

Знак "⇒" здесь означает переход на другую разработку. См. "Генеалогия".

Изображение — логотип статьи

К зашифрованным файлам добавляется случайное расширение: **.<random>**

Примеры таких расширений:
.BuchX
.SNwyR
.cyekE

В обновленном варианте стало использоваться расширение: **.tx_locked**
(т.е. "ThunderX locked").

Позже, вариант Ranzy Locker получил расширения **.RNZ и .ranzy**

Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Ранняя активность этого крипто-вымогателя пришлась на конец августа - начало сентября 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **readme.txt**

Содержание записки о выкупе (1-й вариант):
Attention! Your network has been locked
All files on each host has been encrypted
For this server all encrypted files have extension: .SNwyR

You cant open or work with encrypted files while it encrypted
All backups has been deleted or formatted, do not worry, we can help you restore your files
We use strongest encryption algoriths, the only way to return your files back - contact us and receive decryption program.
Do not worry about guarantees - you can decrypt any 3 files FOR FREE as guarantee
---
Contact us: deloneThunder@protonmail.com or ThunderBirdXeX@cock.li
And attach in first letter this file or just send all info below (copy all info!):
key: eyJleHQiOiIuU053eVIiLCJrZXkiOiJKMElr*** [totally 1012 chars]
personal id: AX90F***

Перевод записки на русский язык (1-й вариант):
Внимание! Ваша сеть заблокирована
Все файлы на каждом хосте зашифрованы
Для этого сервера все зашифрованные файлы имеют расширение: .SNwyR

Вы не сможете открыть зашифрованные файлы или работать с ними, пока они зашифрованы
Все резервные копии удалены или отформатированы, не волнуйтесь, мы можем помочь вам вернуть ваши файлы
Мы используем самые надежные алгоритмы шифрования, единственный способ вернуть ваши файлы - написать нам и получить программу дешифрования.
Не беспокойтесь о гарантиях - вы можете БЕСПЛАТНО расшифровать любые 3 файла в качестве гарантии

Пишите нам: deloneThunder@protonmail.com или ThunderBirdXeX@cock.li
И прикрепите в первом письме этот файл или просто отправьте всю инфу ниже (скопируйте всю инфу!):
ключ: eyJleHQiOiIuU053eVIiLCJrZXkiOiJKMElr *** [всего 1012 символов]
персональный id: AX90F ***

Сравните ранний вариант с более новым вариантом записки.

Содержание записки о выкупе (2-й вариант):
Attention! Your network has been locked by ThunderX
Your computers and server are encrypted
For this server all encrypted files have extension: .tx_locked
Follow our instructions below and you will recover all your data
---
You cant open or work with files while it encrypted - we use strongest encryption algorithm ***
All backups are deleted or formatted, do not worry, we can help you restore your files
The only way to return your files back - contact us and receive decryption program.
Do not worry about guarantees - you can decrypt any 3 files FOR FREE as guarantee
---
Contact us: deloneThunder@protonmail.com or ThunderBirdXeX@cock.li
And attach in first letter this file or just send all info below (copy all info!):
key: ***
personal id: ********

Перевод записки на русский язык (2-й вариант):
Внимание! Ваша сеть заблокирована ThunderX
Ваши компьютеры и сервер зашифрованы
Для этого сервера все зашифрованные файлы имеют расширение: .tx_locked.
Следуйте нашим инструкциям ниже, и вы восстановите все свои данные

Вы не можете открывать файлы или работать с ними, пока они зашифрованы - мы используем самый надежный алгоритм шифрования ***
Все резервные копии удалены или отформатированы, не волнуйтесь, мы поможем вам восстановить ваши файлы
Единственный способ вернуть ваши файлы - связаться с нами и получить программу для дешифрования.
Не беспокойтесь о гарантиях - вы можете БЕСПЛАТНО расшифровать любые 3 файла в качестве гарантии

Пишите нам: deloneThunder@protonmail.com или ThunderBirdXeX@cock.li
И прикрепите в первом письме этот файл или просто отправьте всю инфу ниже (скопируйте всю инфу!):
ключ: ***
персональный id: ********

Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

➤ Удаляет теневые копии файлов с помощью команды:
wmic.exe SHADOWCOPY /nointeractive
vssadmin.exe Delete Shadows /All /Quiet

Список файловых расширений, подвергающихся шифрованию:
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Список пропускаемых расширений:

.dll, .exe, .ini, .lnk, .key, .rdp

Пропускаемые директории:
AppData, boot, PerfLogs, PerfBoot, Intel, Microsoft, Windows, Tor Browser.

Файлы, связанные с этим Ransomware:
readme.txt - название файла с требованием выкупа
<random>.exe - случайное название вредоносного файла

LockerStub.pdb - название файла проекта

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

C:\Users\Gh0St\Desktop\ThunderX\Release\LockerStub.pdb

Записи реестра, связанные с этим Ransomware:
См. ниже результаты анализов.

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: deloneThunder@protonmail.com, ThunderBirdXeX@cock.li
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
🔻 **Triage analysis >>**
Ⓗ **Hybrid analysis >>**
Σ **VirusTotal analysis >>** **VT>**
🐞 **Intezer analysis >>** **IA>**
⋟ ANY.RUN analysis >>
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲ JOE Sandbox analysis >>

Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

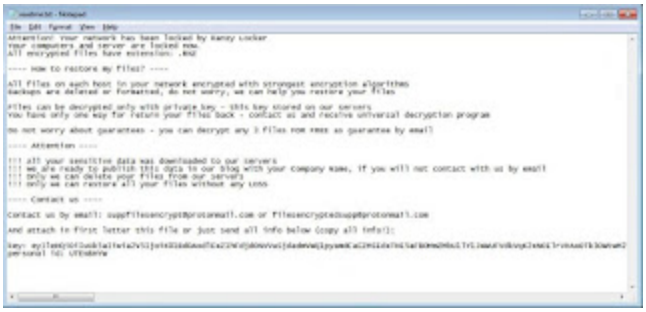
=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Обновление от 7 сентября 2020:
Сообщение >>
Расширение: **.tx_locked**
Записка: readme.txt
Результаты анализов: **VT** + **IA**

Обновление от 14 сентября 2020:
Сообщение >>
Расширение: **.tx_locked**
Записка: readme.txt
Email: mbhelp@protonmail.com
akodesh@tutanota.com
Результаты анализов: **VT** + **VMR** + **IA**

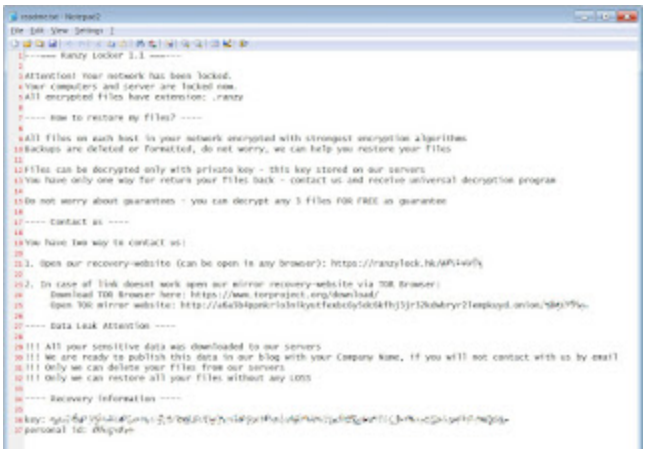
Обновление от 29 сентября 2020:
Сообщение >>
Самоназвание в записке: Ranzy Locker
Название файла проекта: C:\Users\Gh0St\Desktop\ThunderX\Release\LockerStub.pdb
Расширение: **.RNZ**
Записка: readme.txt
Email: suppfilesencrypt@protonmail.com, filesencryptedsupp@protonmail.com
Результаты анализов: **VT** + **IA** + **HA**

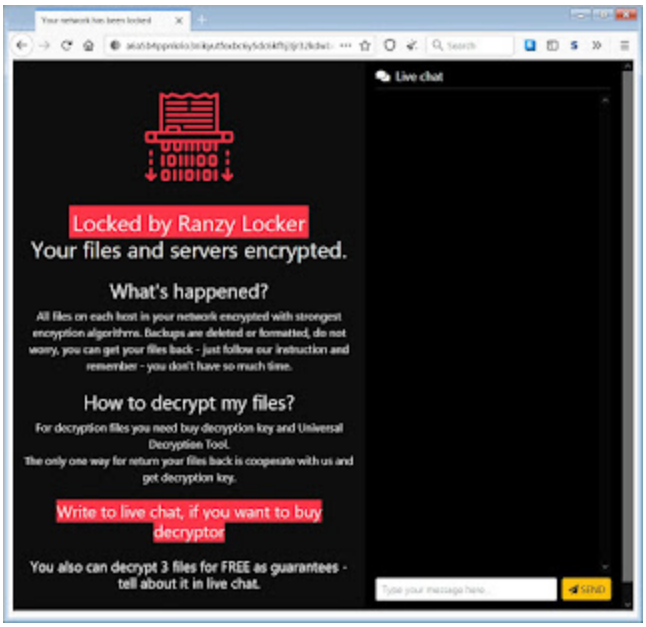


Обновление от 5 октября 2020:
Вымогатели подготовили замену.
Новый образец вредоного ПО: **VT** + **IA**
Дата создания: 5 октября 2020.
Дата загрузки на анализ: 21 октября 2020.
На скриншоте от Intezer видно, что в этом образце есть гены обоих версий.

Обновление от 16 октября 2020:
Статья на сайте BC >>

Расширение: **.ranzy**
Записка: readme.txt
Сайт: hxxxs://ranzylock.hk/***



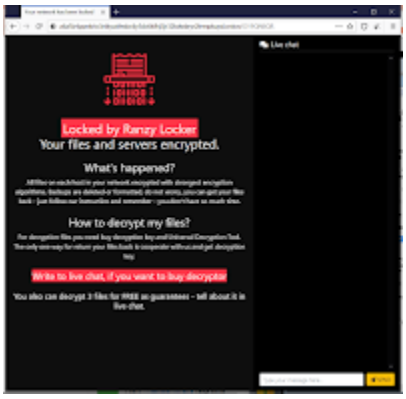


Теперь официально сообщается:
1) этот шифровальщик получил новое название Ranzy Locker;
2) Группа, управляющая Ranzy Locker, запустила сайт "Ranzy Leak" для публикации украденных данных.

Обновление от 16 октября 2020:
Сообщение >>
Версия: Ranzy Locker 1.1
Расширение: **.ranzy**
Теперь используются 2 сайта в сети Tor: один вместо email для общения с жертвами, другой назвается "Ranzy Leak", для публикации украденных данных. Кстати этот домен ранее использовался вымогателями Ako Ransomware.

Обновление от 28 октября 2020:
Сообщение >>
Сообщение >>

Расширение: .ranzy
URL: hxxx://ranzylock.hk/O19QN6QR
Tor-URL: xxxx://a6a5b4ppnkrio3nikyutfexbc6y5dc6kfhj3jr32kdwbryr2lempkuyd.onion/

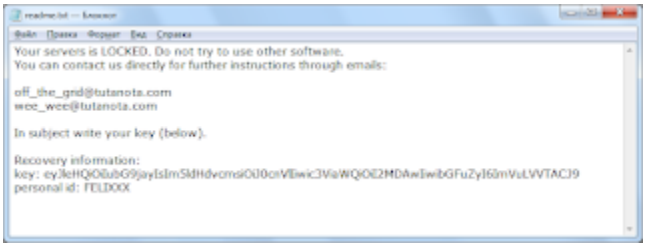


Анализы: **VT** + **IA** / **VT**

Вариант от 22 февраля 2021:
Сообщение >>
Расширение: **.RANZYLOCKED**
Записка: readme.txt
Email: kazinbekdutch@tutanota.com
kazinbekdutch@cock.li
kazinbekdutch@protonmail.com
Результаты анализов: **VT**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33314
BitDefender -> Gen:Heur.Ransom.REntS.Gen.1
ESET-NOD32 -> A Variant Of Win32/Filecoder.RanzyLocker.A
Malwarebytes -> Ransom.Ranzy
Microsoft -> Ransom:Win32/FileCrypter.MB!MTB
Qihoo-360 -> Win32/Ransom.Generic.HwoCdjkA
Rising -> Ransom.FileCrypter!8.11F42 (CLOUD)
Symantec -> ML.Attribute.HighConfidence
Tencent -> Malware.Win32.Gencirc.11b0ebcf
TrendMicro -> Ransom.Win32.RANZYLOCKER.SMTH

Вариант от 12 сентября 2021:
Сообщение >>

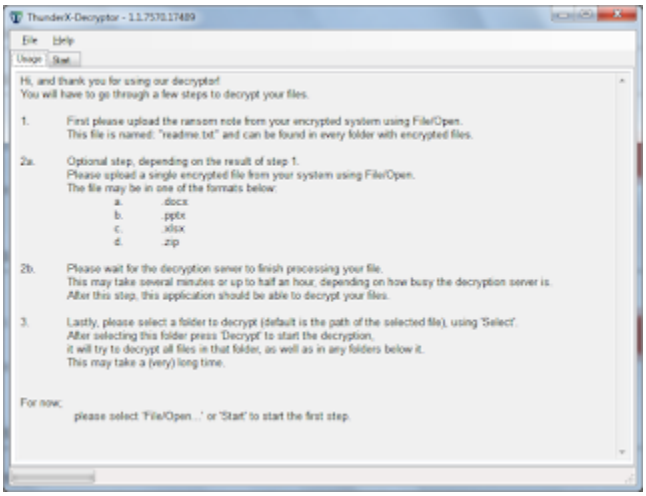
Расширение: .lock
Записка: readme.txt
Email: off_the_grid@tutanota.com, wee_wee@tutanota.com
Результаты анализов: **VT** + **AR**



=== БЛОК ССЫЛОК и СПАСИБОК = BLOCK OF LINKS AND THANKS ===

Внимание!

Файлы, зашифрованные ThunderX, можно дешифровать!
Рекомендую обратиться по этой ссылке к Майклу Джиллеспи >>
***
Или пишите в Tesorion, у них есть бесплатный дешифровщик >>
*



Thanks:

S!Ri, Michael Gillespie
Andrew Ivanov (author)
Tesorion
to the victims who sent the samples